UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/492,273	01/27/2000	Wolfgang Rankl	JEK/Rankl	9676

7590 04/11/2006

J. Ernest Kenney
Bacon & Thomas PLLC
625 Slaters Lane
4th Floor
Alexandria, VA 22314-1176

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/492,273	RANKL, WOLFGANG	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 3/8/2006 was received and considered.

2. Claims 1-9 are pending.

Response to Arguments

3. In view of the appeal brief filed on 3/8/2006, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below: JCJ 4/5/06

Claim Objections

4. Claims 1-9 are objected to because of the following informalities:

Regarding claim 1, "on exchange" (line 4) should be replaced with "an exchange".

Regarding claims 1 & 3, the bulleting should be removed to put the claims in the recognized proper format.

Regarding claim 3, the claim should end with a period (.).

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 1, the limitation "the secret initial value" (line 4) lacks proper antecedent basis.

Regarding claim 3, the limitation "the part of the first values generated" (lines 3-4) lacks proper antecedent basis.

Regarding claim 3, the phrase "in particular" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1 & 3-5 are rejected under 35 U.S.C. 102(b) as being anticipated by "Smart Card Tutorial - Integrated Circuit Card Standards and Specifications – Part 10" by **Everett**.

Regarding claim 1, Everett discloses inserting a chip card/smart card into a processing station/EFTPOS (p. 4, ¶1), and initializing the chip card/smart card by having the processing station and the chip card each determine the secret initial value/ $a^{xy} \bmod p$ based on exchange of parts of first and second values generated ($x, a^x \bmod p$, y , $a^y \bmod p$), respectively, in the processing station/correspondent A and the chip card/correspondent B (Fig. 2), wherein first values/($x, a^x \bmod p$) for determining the secret initial value/ $a^{xy} \bmod p$ (Fig. 2) are generated in the processing station/correspondent A (Fig. 2), parts of the first values/($x, a^x \bmod p$) are transmitted to the chip card/correspondent B (Fig. 2), second values/(y , $a^y \bmod p$) for determining the secret initial value/ $a^{xy} \bmod p$ are generated in the chip card/correspondent B, parts of the second values/(y , $a^y \bmod p$) are transmitted to the processing station/correspondent A (Fig. 2), the secret initial value/ $a^{xy} \bmod p$ is determined from at least parts of the first values/ x and the transmitted parts of the second values/ $a^y \bmod p$ (Fig. 2) and the secret initial value/ $a^{xy} \bmod p$ is determined from at least parts of the second values/ y and the transmitted parts of the first values/ $a^x \bmod p$ (Fig. 2).

Regarding claims 3-5, Everett discloses the first values generated in the processing station/ x are subjected to a first function/ $a^x \bmod p$ (Fig. 2), the result of the first function is transmitted to the chip card/correspondent B in addition to the part of the first values

generated/ $a^x \bmod p$ (Fig. 2), at least one part of the second values generated in the chip card/ y is subjected to a second function/ $a^y \bmod p$ with the transmitted part of the first values/ y, the secret initial value/ $a^{xy} \bmod p$ is generated in the processing station/correspondent A by means of a third function/ $\left(a^y\right)^x \bmod p$ from the transmitted result of the second function/ $a^y \bmod p$ and a part of the first values/ x, in particular the first part of the values not transmitted to the chip card/ x (Fig. 2) and the secret initial value/ $a^{xy} \bmod p$ is generated in the chip card/correspondent B by means of a fourth function/ $\left(a^y\right)^x \bmod p$ from the transmitted result of the first function/ $a^x \bmod p$, the transmitted part of the first values/ $a^x \bmod p$ and a part of the second values not transmitted to the processing station/ y (Fig. 2).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Everett**, as applied to claim 1 above, in further in view of "Cryptographic Identification Methods for Smart Cards in the Process of Standardization" by Hans-Peter **Königs** in further view of Handbook of Applied Cryptography by **Menezes**. Schneier discloses a system, as modified above, but lacks using an individual identifier to generate the initial value for the card. Königs teaches that one can greatly

simplify the problem of key management and make an explicit public key unnecessary by deducing a verification key from an identification word/individual identifier (see page 46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Everett's system to use identification information as the basis for a key. One of ordinary skill in the art would have been motivated to perform such a modification to simplify key management, as taught by Königs (see page 46). Everett, as modified above, lacks the identification information being a serial number. However, Menezes teaches that sequence numbers can be used to identify entities, often in key establishment protocols (see §10.3.1 & §10.12). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Everett to use the serial number of the smart card for identification, and hence as the basis for the key. One of ordinary skill in the art would have been motivated to perform such a modification to provide uniqueness, as taught by Menezes (see §10.3.1 & §10.12).

11. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Everett**, as applied to claim 1 above, and further in view of U.S. Patent 5,452,358 to Normile et al. (**Normile**). Schneier, as applied to claim 1, does not disclose using the secret initial value as the start value for generating random numbers. However, Normile teaches that a secret key can be used as a seed value for generating random numbers, which can then be used to encrypt data (col. 4, lines 9-20). Further, Schneier teaches that good keys are random strings, i.e. a key used for encryption should be, at least to some degree, random (pages 173-174). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify

Everett to use the secret initial value as a start value for generating random numbers. One of ordinary skill in the art would have been motivated to perform such a modification to add randomness to the keys used for encryption, as taught by Schneier (pages 173-174) and Normile (col. 4, lines 9-20).

12. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Everett**. Everett lacks explicitly disclose encrypting and decrypting data with the key. However, the examiner takes Official Notice that using a secret key for encryption is old and well established in the art of cryptography as a method of protecting data. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Everett to use the secret initial value for encrypting and decrypting data. One of ordinary skill in the art would have been motivated to perform such a modification to protect data from eavesdroppers. This advantage is well known to those skilled in the art.

13. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Everett**, as applied to claim 1 above, in further view of Applied Cryptography, Second Edition by **Schneier** and U.S. Patent 6,038,551 to Barlow et al. (**Barlow**). Everett's system lacks transmission of additional keys to the card. However, Barlow teaches that to support multiple applications, the card must enable a user to transport keys from one application to another (col. 4, lines 34-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Everett's system to allow multiple keys to be transported to the chip card. One of ordinary skill in the art would have been motivated to perform such a

modification to support multiple applications, as taught by Barlow (col. 4, lines 34-49). As modified, Everett's system encrypting and decrypting further secret keys using the key generated in the processing station and the chip card. However, Schneier teaches that keys also need to be cryptographically protected during transport and that it is common to encrypt data keys (keys for encrypting data) with key encrypting keys for transfer (p. 176-177, §8.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Everett, as modified above, to cryptographically protect the keys in transport using the key generated in the processing station and the chip card. One of ordinary skill in the art would have been motivated to perform such a modification to protect the keys during transport, as taught by Schneier (p. 176-177, §8.3).

14. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Everett, Schneier** and **Barlow**, as applied to claim 8 above, and further in view of U.S. Patent 5,224,163 to Gasser et al. (**Gasser**). Everett's system, as modified above, lacks removal of the original session key after the receipt of personalization information. Gasser teaches that removing a key after it's use in an authorization system ensures security even if one of the participants is compromised thereafter (see col. 15, lines 51-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Everett to remove the session key from Everett's system after the initial transaction was complete. One of ordinary skill in the art would have been motivated to perform such a modification to prevent compromise of both the card and the apparatus if either was compromised, as taught by Gasser (see col. 15, lines 51-65).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached at (571) 272-6962.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS

March 28, 2006